The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED:
8/1/2013

SUBJECT:
McAfee Artemis/GTI File Reputation producing false-positives

Overview:
McAfee has reported that their Artemis/GTI File Reputation within ePolicy Orchestrator (ePO) is reportedly flagging Windows and other legitimate files as malware. McAfee ePO is an enterprise management platform for anti-virus and host intrusion prevention systems. This issue may cause system errors or prevent Windows from starting. Organizations utilizing McAfee ePO are advised to review client systems for errors. Errors found or Windows system files in quarantine may indicate the organization is impacted.

Systems Affected:

- McAfee ePolicy Orchestrator

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

Description:
McAfee has reported that their Global Threat Intelligence (GTI) Artemis File Reputation within ePolicy Orchestrator (ePO) is reporting false positives. As a result legitimate files, such as Windows system files, are being identified as malicious and are being incorrectly quarantined. The GTI servers causing the issue have been taken off line. However, environments with a GTI proxy may still have affected files cached.

Please note this is not an issue with the current McAfee DAT files.

Recommendations:

The following actions should be taken:

- If your organization has been affected, DO NOT RESTART the system as it could result in the files being permanently unrecoverable.
- Consider implementing the workarounds provided by McAfee (https://kc.mcafee.com/corporate/index?page=content&id=KB78993) in your environment:
  - Use the Quarantine Restore Tool to recover files that have been incorrectly
  - detected and quarantined. The recovery tool will restore the detections contained within the On-Access and On-Demand scan logs during the period of the disruption.
  - The GTI servers that caused this issue have been taken offline and the issue
  - will not recur.
  - Restore files locally through the VirusScan Enterprise (VSE) 8.x Console:
  - Create an ePolicy Orchestrator (ePO) task to restore quarantined items.
- Organizations that are running EPO may also take preventive measures by turning off heuristics.

References:

McAfee:

https://kc.mcafee.com/corporate/index?page=content&id=KB78993

SANS:

http://isc.sans.edu/diary/16264